

Mini-Switch in Alcatel-Lucent IP-Touch Telephones Allows Un-Authenticated Access to Voice VLAN

Summary

Insecure default configurations in Release 7.0 and later of Alcatel-Lucent's Voice-over-IP Telephone System OmniPCX Enterprise can be exploited to gain un-authenticated access to the voice VLAN through daisy chained computer systems.

This vulnerability is tracked as Alcatel-Lucent defect number XTSce69338

(optionally) CVSS Score (base metrics only) : (including steps how this number was achieved)

CVSS Base score	7.0
Access Vector	Remote
Access Complexity	Low
Authentication	Not Required
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	Partial
Impact Bias	Availability

History

Date of notification : 23nov2005

Date of creation : Ed.01 (14feb2007)

Affected Products and Configurations

All version of OmniPCX Enterprise supporting 802.1x authentication (release R7.0 and later) can be configured so that:

- the IP Touch mini switch PC port is not authorized, and consequently no device can be chained behind the terminal, or;
- the IP Touch mini switch filters VLAN tagged frames, preventing the device chained behind the terminal to send Voice VLAN tagged frames and receive multicast or broadcast Voice VLAN tagged frames or;
- the IP Touch phone internal switch does not filter VLAN tagged frames, thereby allowing the device chained behind the terminal to send frames tagged in the Voice VLAN and receive multicast or broadcast frames tagged in the Voice VLAN.

By default the PC port is enabled without VLAN filtering. This configuration can be modified with the OmniPCX Enterprise management interface (mgr command line tool or OmniVista 4760, Phone Class of Service, value 'State PC Port').

Detailed description

To successfully attack an infrastructure the following requirements must be met:

- Physical access to the built-in mini switch in an Alcatel-Lucent IP Touch telephone
- Improper configuration of the PC port state on the IP Touch's mini switch
- 801.1q VLAN segmentation must be used to separate the "voice network" from other networks
- 802.1x authentication must be enabled to authenticate telephones and control their access to the voice VLAN



The two port internal mini switch of the IP Touch terminals is enabled, by default, in a vulnerable configuration that does not filter Voice VLAN tagged frames unless a proper configuration action is performed. Thus, Voice VLAN multicast and broadcast frames coming from the network are sent to the PC port, and voice VLAN frames coming from the PC port are forwarded to the network. This allows a device chained to the IP touch phone to access the Voice VLAN.

When the 802.1x authentication has been activated on the IP Touch, and the switch port is configured in multiple access mode, the device plugged behind the IP Touch's mini switch PC port is not authenticated, and the terminal vulnerability allows it to intrude the Voice VLAN although the 802.1x authentication's purpose was to guarantee VLAN isolation.

When no network access authentication is implemented, this problem is less relevant as there are easier ways of plugging an unauthorized device on a Voice VLAN port of a switch.

Impact of the vulnerability

Access to the voice VLAN from an unauthorized device can be used as a channel for denial of service or VoIP device impersonations attacks.

Solutions

Workaround

Customers with Alcatel-Lucent's switches are advised to follow these good practice recommendations:

- The IEEE 802.1X function (multi-client and multi-VLAN) must be enabled whenever possible to avoid unauthorized access as it allows to authenticate every device/user connected on the same Ethernet switch port.
For the availability of this feature and his configuration, see the boilerplate regarding your model and AOS version or contact your business partner.

To avoid a disconnection of authenticated equipments by an attacker, we recommends also to enable the re-authentication 802.1X. After a client 802.1X (supplicant) has successfully authenticated through an 802.1X port, the switch may be configured to periodically re-authenticate the supplicant (re-authentication is disabled by default). The re-authentication process is transparent to a user connected to the authorized port. The process is used for security and allows the authenticator (the OmniSwitch) to maintain the 802.1X connection

- When the full authentication by 802.1X for the IP Touch and the PC is not possible, the customer can configure different device classification policies for a 802.1X client (IP Touch) and a non 802.1X client (Pc) on the same physical port. These security policies could be:
 - 802.1X authentication—performs 802.1X authentication via a remote RADIUS server.
 - MAC authentications—performs MAC based authentication via a remote RADIUS server.
 - Group Mobility rules—uses Group Mobility rules to determine the VLAN assignment for a device
 - VLAN ID—assigns the device to the specified VLAN.
 - Default VLAN—assigns a device to the default VLAN for the 802.1X port.
 - Block—blocks a device from accessing the 802.1X port.

For additional policies and configuration, see the boilerplate regarding your model and AOS version or contact your business partner.

- For the critical devices like the Communication Server etc. Alcatel-Lucent strongly recommends to create a dedicated VLAN for all the critical servers of the Enterprise. This VLAN is secured by multiple ways like:



- A Brick Firewall that filters and authorizes the flows between this critical VLAN and the others VLANs;
- A device based on Intrusion Prevention (IPS) like the OmniAccess Safeguard or Intrusion Detection (IDS) like the Fortigate / Snort could help to prevent DoS attacks;
- A Quarantine Manager, in association with the IPS/IDS, could be a solution to react in real-time against the IP attacks.

For the customers with others vendor's switches, please contact your reseller. As some competitors don't support yet the 802.1X authentication for multiple clients/multi-VLAN on their switches, it's very difficult to have a good solution to authenticate all the devices connected on the same port.

- Port security can be used to limit access on an Ethernet port based on the MAC address of the device to which it is connected. It also can be used to limit the total number of devices plugged into a switch port. (For additional solutions and configurations, please contact your reseller).
- With a 802.1X port, the customer could associate a guest VLAN, clients that are not 802.1X-capable are put into this dedicated VLAN with a restricted access to the network. (For additional solutions and configurations, please contact your reseller).
- For the critical devices like the Communication Server etc. Alcatel-Lucent strongly recommends to create a dedicated VLAN for all the critical servers of the Enterprise, this VLAN could be secured by multiple ways like:
 - Access Control Lists can be used to restrict access to sensitive portions of the network by filtering packets based on source and destination MAC addresses, IP addresses, or TCP/User Datagram Protocol (UDP) ports;
 - Secure with a Brick Firewall for the filtering and the authorization for the protocols between all the VLANs;
 - Use some IPS/IDS (Snort/Fortigate) in conjunction with the Quarantine Manager for automatic answers against the IP attacks.

Fixed Software Versions and how to obtain them

All OmniPCX Enterprise Release 7.0 and later support 802.1x authentication and the configuration option for the mini switch PC port which shall be securely configured.

References

RUS-CERT web site : [2007-06:01 \(1380\)](#)

CVE entry number : [CVE-2007-2512](#)

Vendor Statement

ALU is committed to continuously enhancing our security posture, and we have both internal and external resources involved in security review processes aimed at identifying product vulnerabilities, both in existing and in developing products.

It is important to note that there have been no reports of compromise due to this vulnerability. ALU's primary concern in this instance is to rapidly deploy a solution for our entire customer base. As a result, ALU has released patches for most code versions.

While we encourage customers to always utilize the latest releases to ensure the full benefit of our continued innovation and improvements, we recognize that this is not always possible.

Information on our disclosure policy, how to report vulnerabilities can be found [here](#).